G 7 3 9

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-331375
(43)Date of publication of application : 30.11.2001

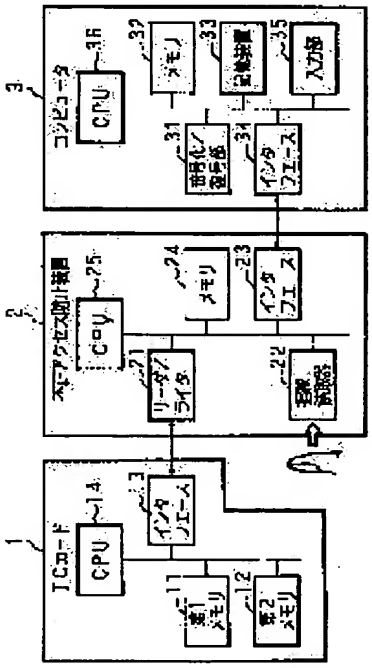
(51)Int.Cl. G06F 12/14
G06F 3/06
G06F 3/08
G06F 9/445
G06F 1/00
G06F 12/00
G06K 19/10
G06K 19/00
H04L 9/32

(21)Application number : 2000-151808
(22)Date of filing : 23.05.2000

(71)Applicant : NIPPON LSI CARD CO LTD
(72)Inventor : OKI SHINJI

(54) PROGRAM STARTUP METHOD, METHOD AND DEVICE FOR PREVENTING UNAUTHORIZED ACCESS, ENCODING/DECODING SYSTEM AND CARD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and a device, capable of preventing an unauthorized user from accessing a storage device in which data is stored at an encoded state by pretending to be someone else.
SOLUTION: Fingerprints of a user to access the storage device 33 in a computer 3 are read by a fingerprint reader 22, data about prescribed fingerprint information stored in a first memory 11 of an IC card 1 are collated with the read fingerprint information, operation algorithm for encoding/decoding stored in a memory 32 is started, only when both pieces of fingerprint information match each other, the data to be stored in the storage device 33 is encoded by an encoding/decoding part 31 and encoded data stored in the storage device 33 is decoded simultaneously.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－331375
（P2001－331375A）
(43)公開日　平成13年11月30日(2001.11.30)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
3/06	３０４	3/06	３０４Ｈ	５Ｂ０３５
3/08		3/08	Ｃ	５Ｂ０６５
9/445		12/00	５３７Ｄ	５Ｂ０７６
1/00		9/06	６５０Ｄ	５Ｂ０８２

審査請求　未請求　請求項の数８　ＯＬ　（全 ９ 頁）　最終頁に続く

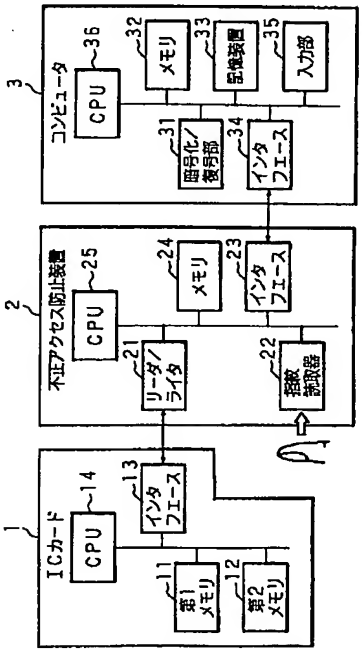
(21)出願番号　特願2000－151808(P2000－151808)
(22)出願日　平成12年５月23日(2000.5.23)

(71)出願人　000228132
日本エルエスアイカード株式会社
大阪市浪速区日本橋５丁目１番19号
(72)発明者　大木　信二
大阪府松原市南新町１丁目12番25－609号
(74)代理人　100078868
弁理士　河野　登夫

Ｆターム(参考)　5B017 AA07 BA07 BA09 CA07 CA14
5B035 AA14 BB09 BC01
5B065 BA01 BA09 CA40 PA16
5B076 FB05
5B082 EA11 GA11
5J104 AA07 KA01 KA16 KA17 NA33
NA38

(54)【発明の名称】　プログラム起動方法、不正アクセス防止方法及び装置、暗号化／復号システム並びにカード

(57)【要約】
【課題】　不正なユーザが他人になりすまして、暗号化した状態でデータが記憶される記憶装置へアクセスすることを防止できる方法及び装置を提供する。
【解決手段】　コンピュータ３内の記憶装置３３にアクセスするユーザの指紋を指紋読取器２２にて読み取り、ＩＣカード１の第１メモリ１１に格納されている所定の指紋情報のデータとその読み取った指紋情報とを照合し、一致した場合にのみ、メモリ３２に格納されている暗号化用／復号用の動作アルゴリズムが起動されて、暗号化／復号部３１にて記憶装置３３に記憶すべきデータを暗号化すると共に記憶装置３３に記憶されている暗号化データを復号する。



【特許請求の範囲】

【請求項１】　データを暗号化する動作プログラム、及び／または、暗号化されたデータを復号する動作プログラムを、所定の暗証にて起動する方法において、前記暗証として身体的特徴を用いることを特徴とするプログラム起動方法。

【請求項２】　前記身体的特徴は指紋である請求項１記載のプログラム起動方法。

【請求項３】　暗号化した状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する方法において、前記記憶装置にアクセスしたユーザの身体的特徴を得る第１ステップと、得た身体的特徴と所定の身体的特徴とを照合する第２ステップと、前記両身体的特徴が一致した場合に、前記記憶装置に記憶すべきデータを暗号化する動作プログラム、及び／または、前記記憶装置に記憶されている暗号化データを復号する動作プログラムを実行する第３ステップとを有することを特徴とする不正アクセス防止方法。

【請求項４】　前記所定の身体的特徴はカードに書き込まれており、前記第２ステップにおいて、前記カードから前記所定の身体的特徴を読み出し、読み出した前記所定の身体的特徴と前記第１ステップで得た身体的特徴とを照合する請求項３記載の不正アクセス防止方法。

【請求項５】　暗号化した状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する装置において、前記記憶装置にアクセスしたユーザの身体的特徴を取得する取得手段と、取得した身体的特徴と所定の身体的特徴とを照合する照合手段と、前記両身体的特徴が一致した場合に、前記記憶装置に記憶すべきデータを暗号化する動作プログラム、及び／または、前記記憶装置に記憶されている暗号化データを復号する動作プログラムの実行を許可する許可手段とを備えることを特徴とする不正アクセス防止装置。

【請求項６】　前記取得手段の故障を検知する検知手段と、前記取得手段が故障した場合に、暗証の入力を受け付ける受付手段とを備え、入力された暗証が所定の暗証に一致する場合に、前記許可手段は、前記暗号化する動作プログラム、及び／または、前記復号する動作プログラムの実行を許可すべくなしてある請求項５記載の不正アクセス防止装置。

【請求項７】　暗号化した状態でデータを記憶する記憶装置と、前記記憶装置に記憶すべきデータを暗号化する暗号化手段と、前記記憶装置に記憶されている暗号化データを復号する復号手段と、前記記憶装置にアクセスしたユーザの身体的特徴を取得する取得手段と、取得した身体的特徴と所定の身体的特徴とを照合する照合手段と、前記照合手段での照合によって前記両身体的特徴が一致した場合に、前記暗号化手段及び／または前記復号手段での処理の実行を許可する許可手段とを備えることを特徴とする暗号化／復号システム。

【請求項８】　請求項１～４の何れかに記載の方法に用いられるカードであって、前記所定の身体的特徴が書き込まれていることを特徴とするカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データを暗号化する動作プログラム及び／または暗号化されたデータを復号する動作プログラムの起動を制御するプログラム起動方法、暗号化された状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する方法・装置及び暗号化／復号システム、並びに、これらの方法に使用するカードに関する。

【０００２】

【従来の技術】コンピュータは、ノート型コンピュータに代表されるように、小型化及び可搬化が進んでいる。このような小型のコンピュータにあっても、小型で大容量のハードディスクの搭載により、大量のデータを内部に記憶することができる。また、そのデータを記憶しておくハードディスクにあっては、既存の固定型のものから、高密度実装技術の発展に伴って今後はカード形式の可搬型のものの開発も進行している。

【０００３】このような各デバイスの小型化，軽量化が図られていく状況にあって、ノート型コンピュータ本体または可搬型ハードディスクが盗難されて、ハードディスクに記憶されているデータが漏洩または改竄される事態を防止することは重要な問題である。そこで、データをそのままハードディスクに記憶しておくのではなく、記憶すべきデータを暗号化した後にハードディスクに記憶することが一般的に行われれている。

【０００４】データを暗号化する処理，暗号化されたデータを復号する処理は、夫々、既存の暗号化用の動作プログラム，復号用の動作プログラムに従ってソフトウェア的に行われるが、それらの処理が不正なユーザによってなされないように、各動作プログラムの起動には特定の数字，文字等からなる暗証情報の入力を必要としている。つまり、正しい暗証情報が入力された場合にのみ、これらの暗号化用及び／または復号用の動作プログラムが起動して、ハードディスクにアクセスできるようにしており、これによってノート型コンピュータ本体または可搬型ハードディスクが盗難されても、それらへの不正なアクセスを防止して記憶データの漏洩，改竄を防いでいる。

【０００５】

【発明が解決しようとする課題】しかしながら、上述した従来の方式では、暗号化用及び／または復号用の動作プログラムを起動させるための暗証情報が数字，文字等にて構成されているので、それが漏洩する可能性もあり、漏洩された場合には不正なユーザがその漏洩暗証情報を用いて容易にそれらの動作プログラムを起動してハードディスクにアクセスすることが可能となり、安全性

が十分ではないという問題がある。

【０００６】本発明は斯かる事情に鑑みてなされたものであり、取得した身体的特徴と所定の身体的特徴とを照合して一致した場合に、暗号化用の動作プログラム及び／または復号用の動作プログラムを起動することにより、不正なユーザが他人になりすまして不正に暗号化処理及び／または復号処理を行うことを防止できて従来例よりも安全性を高くできるプログラム起動方法を提供することを目的とする。

【０００７】本発明の他の目的は、取得した身体的特徴と所定の身体的特徴とを照合して一致した場合に、暗号化用の動作プログラム及び／または復号用の動作プログラムを起動して記憶装置へのアクセスを可能とすることにより、不正なユーザが他人になりすまして不正に記憶装置へアクセスすることを防止できる不正アクセス防止方法及び装置を提供することにある。

【０００８】本発明の更に他の目的は、不正なユーザによる暗号化処理及び／または復号処理を防止できる暗号化／復号システムを提供することにある。

【０００９】本発明の更に他の目的は、上記のような方法に使用するカードを提供することにある。

【００１０】

【課題を解決するための手段】請求項１に係るプログラム起動方法は、データを暗号化する動作プログラム、及び／または、暗号化されたデータを復号する動作プログラムを、所定の暗証にて起動する方法において、前記暗証として身体的特徴を用いることを特徴とする。

【００１１】第１発明のプログラム起動方法にあっては、暗号化用の動作プログラム及び／または復号用の動作プログラムを起動するための暗証として身体的特徴を用いる。身体的特徴は各ユーザにおいて固有のものであるので、他人になりすますことは不可能であり、安全性は極めて強固となる。

【００１２】請求項２に係るプログラム起動方法は、請求項１において、前記身体的特徴は指紋であることを特徴とする。

【００１３】第２発明のプログラム起動方法にあっては、身体的特徴として指紋を使用する。身体的特徴となる指紋の取得は容易であって本発明の方法を簡便に行えると共に、指紋は完全に個人を特定できて安全性は極めて高い。

【００１４】請求項３に係る不正アクセス防止方法は、暗号化した状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する方法において、前記記憶装置にアクセスしたユーザの身体的特徴を得る第１ステップと、得た身体的特徴と所定の身体的特徴とを照合する第２ステップと、前記両身体的特徴が一致した場合に、前記記憶装置に記憶すべきデータを暗号化する動作プログラム、及び／または、前記記憶装置に記憶されている暗号化データを復号する動作プログラムを実行する第３ステップとを有することを特徴とする。

【００１５】第３発明の不正アクセス防止方法にあっては、記憶装置にアクセスしようとするユーザの身体的特徴を取得し、その身体的特徴が所定の身体的特徴と一致するか否かを判定し、一致した場合にのみ、記憶装置に記憶すべきデータを暗号化する動作プログラム及び／または記憶装置に記憶されている暗号化データを復号する動作プログラムの起動を可能とする。身体的特徴は各ユーザにおいて固有のものであり、不正なユーザが他人になりすまして記憶装置にアクセスすることは不可能であり、記憶装置の安全性は極めて強固となる。

【００１６】請求項４に係る不正アクセス防止方法は、請求項３において、前記所定の身体的特徴はカードに書き込まれており、前記第２ステップにおいて、前記カードから前記所定の身体的特徴を読み出し、読み出した前記所定の身体的特徴と前記第１ステップで得た身体的特徴とを照合することを特徴とする。

【００１７】第４発明の不正アクセス防止方法にあっては、例えばユーザが携帯するカードに書き込まれている所定の身体的特徴と取得した身体的特徴とを照合する。所定の身体的特徴は、正当なユーザが携帯するカードに書き込まれいて、どこか別のところに格納されていないため、その所定の身体的特徴が漏洩される可能性は非常に低くなり、安全性はより向上する。

【００１８】請求項５に係る不正アクセス防止装置は、暗号化した状態でデータを記憶する記憶装置に対する不正なユーザのアクセスを防止する装置において、前記記憶装置にアクセスしたユーザの身体的特徴を取得する取得手段と、取得した身体的特徴と所定の身体的特徴とを照合する照合手段と、前記両身体的特徴が一致した場合に、前記記憶装置に記憶すべきデータを暗号化する動作プログラム、及び／または、前記記憶装置に記憶されている暗号化データを復号する動作プログラムの実行を許可する許可手段とを備えることを特徴とする。

【００１９】第５発明の不正アクセス防止装置にあっては、取得手段が記憶装置にアクセスしたユーザの身体的特徴を取得し、照合手段がその取得した身体的特徴と所定の身体的特徴とを照合し、許可手段が、両身体的特徴が一致した場合に、暗号化処理及び／または復号処理を許可する。身体的特徴は各ユーザにおいて固有のものであり、不正なユーザが他人になりすまして記憶装置にアクセスすることは不可能であり、記憶装置に対する不正アクセスを完全に防止する。

【００２０】請求項６に係る不正アクセス防止装置は、請求項５において、前記取得手段の故障を検知する検知手段と、前記取得手段が故障した場合に、暗証の入力を受け付ける受付手段とを備え、入力された暗証が所定の暗証に一致する場合に、前記許可手段は、前記暗号化する動作プログラム、及び／または、前記復号する動作プログラムの実行を許可すべくなしてあることを特徴とす

る。

【００２１】第６発明の不正アクセス防止装置にあっては、検知手段が取得手段の故障を検知し、受付手段が、取得手段が故障した場合に、アクセスしたユーザから暗証の入力を受け付け、許可手段が、入力された暗証が所定の暗証に一致する場合に、暗号化処理及び／または復号処理を許可する。よって、取得手段が故障したときでも、従来例と同様の安全性を維持しながら、正当なユーザが記憶装置へのアクセスを行える。

【００２２】請求項７に係る暗号化／復号システムは、暗号化した状態でデータを記憶する記憶装置と、前記記憶装置に記憶すべきデータを暗号化する暗号化手段と、前記記憶装置に記憶されている暗号化データを復号する復号手段と、前記記憶装置にアクセスしたユーザの身体的特徴を取得する取得手段と、取得した身体的特徴と所定の身体的特徴とを照合する照合手段と、前記照合手段での照合によって前記両身体的特徴が一致した場合に、前記暗号化手段及び／または前記復号手段での処理の実行を許可する許可手段とを備えることを特徴とする。

【００２３】第７発明の暗号化／復号システムにあっては、取得した身体的特徴と所定の身体的特徴とが一致した場合に、許可手段が、暗号化手段及び／または復号手段での処理の実行を許可する。身体的特徴によって正当なユーザと不当なユーザとが判別され、不正なユーザによる暗号化処理及び／または復号処理は防止される。

【００２４】請求項８に係るカードは、請求項１～４の何れかに記載の方法に用いられるカードであって、前記所定の身体的特徴が書き込まれていることを特徴とする。

【００２５】第８発明のカードにあっては、そこに正当なユーザ特定するための所定の身体的特徴が書き込まれている。よって、その所定の身体的特徴が漏洩される可能性は非常に低くて安全である。

【００２６】

【発明の実施の形態】以下、本発明をその実施の形態を示す図面を参照して具体的に説明する。図１は、本発明における不正アクセス防止方法を利用した暗号化／復号システムの装置構成を示すブロック図である。図１において、１はＩＣカード、２は不正アクセス防止装置、３はコンピュータである。

【００２７】ＩＣカード１はこのコンピュータ３を使用するユーザ毎に発行され、各ユーザは自身固有のＩＣカード１を有する。このＩＣカード１は接触または非接触での情報の書込み／読出し処理が可能なカードである。

【００２８】ＩＣカード１は、所有するユーザの身体的情報である指紋情報のデータを格納する第１メモリ１１と、コンピュータ３でのデータの暗号化／復号処理の動作プログラムの起動に必要な暗証情報のデータを格納する第２メモリ１２と、不正アクセス防止装置２（リーダ／ライタ２１）との間で情報を送受するインタフェース１３と、これらの各機能素子の動作を制御するＣＰＵ１４とを有する。ＩＣカード１の発行時に、指紋情報のデータとこれに対となる暗証情報のデータとが、第１メモリ１１と第２メモリ１２とに夫々書き込まれる。

【００２９】不正アクセス防止装置２は、ＩＣカード１に対して情報の書込み／読出し処理を行うリーダ／ライタ２１と、ユーザの指紋情報を得る指紋読取器２２と、コンピュータ３との間で情報を送受するインタフェース２３と、指紋照合処理等の動作プログラム等を格納しているメモリ２４と、これらの各機能機器の動作を制御すると共に後述するソフトウェアの処理を実行するＣＰＵ２５とを有する。リーダ／ライタ２１は、ＩＣカード１が装填された場合に、そこに格納されている各種のデータ（指紋情報のデータ，暗証情報のデータ等）を読み出し、指紋情報のデータをＣＰＵ２５へ与え、暗証情報のデータをインタフェース２３を介してコンピュータ３へ出力する。指紋読取器２２は、光学的または静電的に指紋を読み取り、読み取った指紋情報をＣＰＵ２５へ与える。

【００３０】上述した第１メモリ１１及び第２メモリ１２には夫々錠がかけられており、各メモリ１１，１２から格納データを読みだす際には夫々の錠を鍵であける必要がある。第１メモリ１１に対する鍵は、リーダ／ライタ２１が有しており、リーダ／ライタ２１に対応する正当なＩＣカード１であることが鍵となって、第１メモリ１１は開錠される。また、第２メモリ１２に対する鍵は、不正アクセス防止装置２が有しており、ＩＣカード１から読み出された指紋情報の格納データと指紋読取器２２にて得られた指紋情報との一致が鍵となって、第２メモリ１２は開錠される。

【００３１】コンピュータ３は、データを暗号化する暗号化処理及び暗号化データを復号する復号処理を行う暗号化／復号部３１と、暗号化用の動作プログラム，復号用の動作プログラム等を格納しているメモリ３２と、データを暗号化された状態で記憶する記憶装置３３と、不正アクセス防止装置２との間で情報を送受するインタフェース３４と、外部入力を受け付ける入力部３５と、これらの各機能部の動作を制御するＣＰＵ３６とを有する。不正アクセス防止装置２からインタフェース３４を介して正しい暗証が入力された場合に、メモリ３２に格納されている暗号化用／復号用のプログラムが暗号化／復号部３１に読み出されて起動し、暗号化処理／復号処理が行われるようになっている。

【００３２】次に、本発明における不正アクセス防止方法における動作について、その手順を示す図２～図５のフローチャートを参照して説明する。

【００３３】まず、指紋情報及び暗証情報の登録処理について説明する。図２は、その処理の動作手順を示すフローチャートである。このコンピュータ３を使用するユーザの指紋を指紋読取器２２にて読み取って指紋情報を

取得し、そのデータをリーダ／ライタ２１にてＩＤカード１の第１メモリ１１に書き込んで格納する（ステップＳ１１）。

【００３４】この際に、ＣＰＵ２５は、制御プログラムによって特定の数字または文字を発生する。このように発生して設定される特定の数字または文字は、そのユーザの指紋情報のデータと対になる暗証情報であり、そのデータをリーダ／ライタ２１にてＩＤカード１の第２メモリ１２に書き込んで格納する（ステップＳ１２）。なお、これらの指紋情報のデータ及び暗証情報のデータを暗号化して格納しておくようにした場合には、セキュリティが向上する。

【００３５】そして、その暗証情報をコンピュータ３に登録する（ステップＳ１３）。また、これらの指紋情報のデータ及び暗証情報のデータを、そのまま、または暗号化して、緊急復元カードにも書き込んで格納しておく（ステップＳ１４）。この緊急復元カードは、指紋読取器２２の故障等によって指紋照合が不可能になった場合のデータ復元の際に利用されるものであり、通常は厳重に保管される。

【００３６】なお、指紋情報及び暗証情報の登録処理を図１に示す構成部材を利用して行う場合について説明したが、図１のシステムとは無関係にこのような登録処理を行うようにしても良い。

【００３７】次に、データを暗号化して記憶装置３３に記憶する暗号化処理について説明する。図３は、その処理の動作手順を示すフローチャートである。コンピュータ３にアクセスしようとするユーザが携帯するＩＤカード１が、リーダ／ライタ２１に装填される（ステップＳ２１）。ＣＰＵ２５は、装填されたＩＤカード１が、そのリーダ／ライタ２１に対応する正規のカードであるか否かを判断する（ステップＳ２２）。正規のカードである場合に（Ｓ２２：ＹＥＳ）、第１メモリ１１の錠が開けられて、そこに格納されている指紋情報のデータがリーダ／ライタ２１にてＣＰＵ２５に読み出される（ステップＳ２３）。正規のカードでないと判断された場合には（Ｓ２２：ＮＯ）、そのまま動作が終了する。

【００３８】指紋読取器２２にて、ユーザの指紋を読み取って指紋情報を得る（ステップＳ２４）。ＣＰＵ２５は、得られた指紋情報と、読み出された指紋情報のデータとを照合して、両者が一致するか否かを判断する（ステップＳ２５）。一致する場合に（Ｓ２５：ＹＥＳ）、第２メモリ１２の錠が開けられて、そこに格納されている暗証情報のデータがリーダ／ライタ２１にて読み出される（ステップＳ２６）。一致しないと判断された場合には（Ｓ２５：ＮＯ）、そのまま動作が終了する。

【００３９】不正アクセス防止装置２に読み出された暗証情報は、インターフェース２３，３４を介してコンピュータ３に送られる。これによって、メモリ３２から暗号化用の動作プログラムが読み出され、暗号化／復号部３１にてその動作プログラムが起動されて、記憶すべきデータに対する暗号化処理が施される（ステップＳ２７）。そして、暗号化されたデータは、記憶装置３３に記憶される（ステップＳ２８）。

【００４０】次に、記憶装置３３に記憶されている暗号化データを復号する復号処理について説明する。図４は、その処理の動作手順を示すフローチャートである。コンピュータ３にアクセスしようとするユーザが携帯するＩＤカード１が、リーダ／ライタ２１に装填される（ステップＳ３１）。ＣＰＵ２５は、装填されたＩＤカード１が、そのリーダ／ライタ２１に対応する正規のカードであるか否かを判断する（ステップＳ３２）。正規のカードである場合に（Ｓ３２：ＹＥＳ）、第１メモリ１１の錠が開けられて、そこに格納されている指紋情報のデータがリーダ／ライタ２１にてＣＰＵ２５に読み出される（ステップＳ３３）。正規のカードでないと判断された場合には（Ｓ３２：ＮＯ）、そのまま動作が終了する。

【００４１】指紋読取器３２にて、ユーザの指紋を読み取って指紋情報を得る（ステップＳ３４）。ＣＰＵ２５は、得られた指紋情報と、読み出された指紋情報のデータとを照合して、両者が一致するか否かを判断する（ステップＳ３５）。一致する場合に（Ｓ３５：ＹＥＳ）、第２メモリ１２の錠が開けられて、そこに格納されている暗証情報のデータがリーダ／ライタ２１にて読み出される（ステップＳ３６）。

【００４２】不正アクセス防止装置２に読み出された暗証情報は、インターフェース２３，３４を介してコンピュータ３に送られる。これによって、メモリ３２から復号用の動作プログラムが読み出され、暗号化／復号部３１にてその動作プログラムが起動されて、記憶装置３３に記憶されている暗号化データに対する復号処理が施される（ステップＳ３７）。そして、復号されたデータが出力される（ステップＳ３８）。

【００４３】指紋読取器３２で得られた指紋情報とＩＣカード１から読み出された指紋情報のデータとが一致しない場合に（Ｓ３５：ＮＯ）、ＣＰＵ２５は、指紋読取器２２が故障しているか否かを判断する（ステップＳ３９）。故障している場合（Ｓ３９：ＹＥＳ）、入力部３５により暗証情報の外部入力を受け付ける（ステップＳ４０）。これによって、復号用の動作プログラムが起動されて、記憶装置３３に記憶されている暗号化データが復号され（Ｓ３７）、復号されたデータが出力される（Ｓ３８）。このように、指紋読取器３２が故障した場合に、その故障を自身で検知して、暗証情報の外部入力により復号処理を行う補助機能を有している。この際、安全性を確保するために、外部入力された暗証情報がコンピュータ３に残存しないようにする。

【００４４】なお、前述した暗号化処理にあっても、指紋情報の一致が見られない場合に、同様に、指紋読取器

２２の故障を検知したときに暗証情報の外部入力を受け付けて、データの暗号化を行えるように構成しても良い。

【００４５】次に、指紋照合が行えなくなった場合の復元処理について説明する。図５は、その処理の動作手順を示すフローチャートである。緊急復元カードに格納されている暗証情報を読み出し、読み出した暗証情報をコンピュータ３に入力部３５を介して入力する（ステップＳ４１）。メモリ３２内の復号用の動作プログラムを起動して、記憶装置３３に記憶されている全ての暗号化データを暗号化／復号部３１にて復号する（ステップＳ４２）。その後、登録されている指紋情報と暗証情報との対を削除する（ステップＳ４３）。よって、例えばユーザの指が損傷して指紋照合が不可能となった場合でも、暗号化データを元のデータに復号することができる。

【００４６】以下、本発明の不正アクセス防止装置をコンピュータに内蔵した実施の形態について説明する。図６は、このような簡易型の実施の形態の第１例における可搬型コンピュータの要部構成を示すブロック図である。この可搬型コンピュータ４は、１チップの集積回路で構成された指紋スキャナ４１と、データを暗号化する暗号化処理及び暗号化データを復号する復号処理を行う暗号化／復号部４２と、暗号化用／復号用の動作プログラム，指紋照合処理の動作プログラム，所定のユーザの指紋情報のデータ等を格納しているメモリ４３と、データを暗号化された状態で記憶する記憶装置４４と、これらの各機能部の動作を制御すると共に後述するソフトウェアの処理を実行するＣＰＵ４５とを有する。この例では、以下に述べるように、指紋の照合結果を直接、暗号化用／復号用の動作プログラムを起動するための暗証情報としている。

【００４７】次に、データを暗号化して記憶装置４４に記憶する暗号化処理について説明する。図７は、その処理の動作手順を示すフローチャートである。コンピュータ３にアクセスしようとするユーザの指紋を指紋スキャナ４１で読み取って指紋情報を得る（ステップＳ５１）。ＣＰＵ４５は、得られた指紋情報とメモリ４３から読み出した所定の指紋情報のデータとを照合して、両者が一致するか否かを判断する（ステップＳ５２）。一致する場合に（Ｓ５２：ＹＥＳ）、メモリ４３から暗号化用の動作プログラムが読み出され、暗号化／復号部４２にてその動作プログラムが起動されて、記憶すべきデータに対する暗号化処理が施される（ステップＳ５３）。そして、暗号化されたデータは、記憶装置４４に記憶される（ステップＳ５４）。一方、一致しない場合には（Ｓ５２：ＮＯ）、動作はそのまま終了する。

【００４８】次に、記憶装置４４に記憶されている暗号化データを復号する復号処理について説明する。図８は、その処理の動作手順を示すフローチャートである。コンピュータ３にアクセスしようとするユーザの指紋を指紋スキャナ４１で読み取って指紋情報を得る（ステップＳ６１）。ＣＰＵ４５は、得られた指紋情報とメモリ４３から読み出した所定の指紋情報のデータとを照合して、両者が一致するか否かを判断する（ステップＳ６２）。一致する場合に（Ｓ６２：ＹＥＳ）、メモリ４３から復号用の動作プログラムが読み出され、暗号化／復号部４２にてその動作プログラムが起動されて、記憶装置４４に記憶されている暗号化データに対する復号処理が施される（ステップＳ６３）。そして、復号されたデータは出力される（ステップＳ６４）。一方、一致しない場合には（Ｓ６２：ＮＯ）、動作はそのまま終了する。

【００４９】図９は、このような簡易型の実施の形態の第２例における可搬型コンピュータの要部構成を示すブロック図である。この可搬型コンピュータ４は、第１例と同様の指紋スキャナ４１及び暗号化／復号部４２と、データを暗号化された状態で記憶する取外し可能な記憶装置５１と、ネットワークとの通信を行う通信部５２と、暗号化用／復号用の動作プログラム，指紋照合処理の動作プログラム，通信部５２での通信処理用の動作プログラム，所定のユーザの指紋情報のデータ等を格納しているメモリ５３と、これらの各機能部の動作を制御すると共に上述したようなソフトウェアの処理を実行するＣＰＵ５４とを有する。この例では、記憶装置５１が、可搬型コンピュータ４に着脱可能なカード型の可搬型記憶装置である。

【００５０】この第２例でも、暗号化用／復号用の動作プログラムを起動するための暗証情報として指紋の照合結果を用いており、第２例における暗号化処理／復号処理は第１例の場合と同様である。

【００５１】また、第２例では、通信部５２での通信処理の実行には、正当なユーザであるか否かの認証を必要とする。そして、この正当なユーザであるか否かの判断に、暗号化用／復号用の動作プログラムの起動時と同様に、指紋の照合結果を用いる。

【００５２】なお．上述した実施の形態では、身体的特徴として指紋を用いる場合について説明したが、本発明はこれに限らず、掌紋，アイリス，声紋，顔の特徴等、他の身体的特徴を用いることも可能であることは勿論である。

【００５３】また、１人のユーザが１台のコンピュータの記憶装置にアクセスできるようにした例について説明したが、本発明はこれに限らず、特定の複数のユーザがアクセスできるようにも構成できることはいうまでもない。

【００５４】

【発明の効果】以上のように第１発明のプログラム起動方法では、暗号化用の動作プログラム及び／または復号用の動作プログラムの起動用の暗証として、各ユーザにおいて固有のものである身体的特徴を用いるようにした

ので、他人になりすますことは不可能であり、極めて高い安全性を実現できる。

【００５５】第２発明のプログラム起動方法では、身体的特徴として指紋情報を使用するようにしたので、容易に身体的特徴を取得でき、正確かつ簡便に正規のユーザを特定することが可能である。

【００５６】第３発明の不正アクセス防止方法では、ユーザの身体的特徴が所定の身体的特徴と一致するか否かを判定し、一致した場合にのみ、記憶装置に記憶すべきデータを暗号化する動作プログラム及び／または記憶装置に記憶されている暗号化データを復号する動作プログラムの起動を可能とするようにしたので、不正なユーザが他人になりすまして記憶装置にアクセスすることは不可能であり、記憶装置へのアクセスに関して極めて高い安全性を実現できる。

【００５７】第４発明の不正アクセス防止方法では、カードに書き込まれている所定の身体的特徴と取得した身体的特徴とを照合するようにしたので、その所定の身体的特徴が漏洩される可能性は非常に低くなり、安全性をより向上できる。

【００５８】第５発明の不正アクセス防止装置では、取得した身体的特徴と所定の身体的特徴とが一致した場合に、暗号化処理及び／または復号処理を許可するようにしたので、不正なユーザが他人になりすまして記憶装置にアクセスすることは不可能であり、記憶装置に対する不正アクセスを完全に防止することができる。

【００５９】第６発明の不正アクセス防止装置では、身体的特徴を取得する取得手段の故障を検知した場合に、暗証の入力を受け付けるようにしたので、取得手段が故障したときでも、従来例と同様の安全性を維持しながら、正当なユーザが記憶装置へのアクセスを行うことができる。

【００６０】第７発明の暗号化／復号システムでは、取得した身体的特徴と所定の身体的特徴とが一致した場合に、暗号化手段及び／または復号手段での処理の実行を許可するようにしたので、身体的特徴によって正当なユーザと不当なユーザとを容易に判別でき、不正なユーザによる暗号化処理及び／または復号処理を完全に防止できる。

【００６１】第８発明のカードでは、正当なユーザ特定するための所定の身体的特徴が書き込まれるようにしたので、その所定の身体的特徴が漏洩される可能性は非常に低くて安全である。

【図面の簡単な説明】

【図１】本発明における不正アクセス防止方法を利用した暗号化／復号システムの装置構成を示すブロック図である。

【図２】指紋情報及び暗証情報の登録処理の動作手順を示すフローチャートである。

【図３】暗号化処理の動作手順を示すフローチャートである。

【図４】復号処理の動作手順を示すフローチャートである。

【図５】指紋照合が行えなくなった場合の復元処理の動作手順を示すフローチャートである。

【図６】本発明の不正アクセス防止装置をコンピュータに内蔵した第１例の要部構成を示すブロック図である。

【図７】暗号化処理の動作手順を示すフローチャートである。

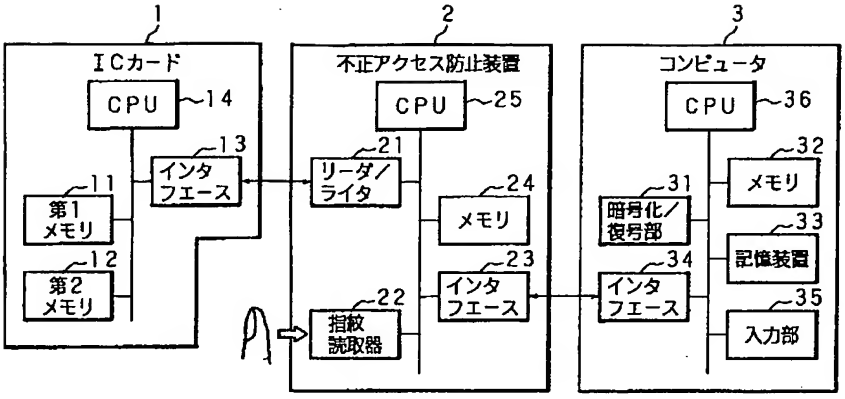
【図８】復号処理の動作手順を示すフローチャートである。

【図９】本発明の不正アクセス防止装置をコンピュータに内蔵した第２例の要部構成を示すブロック図である。

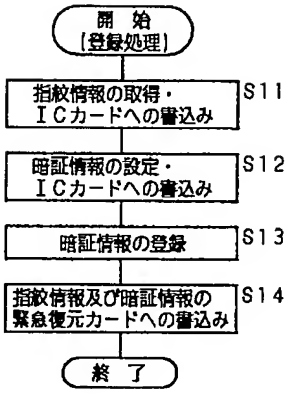
【符号の説明】

１　ＩＣカード
２　不正アクセス防止装置
３　コンピュータ
４　可搬型コンピュータ
１１　第１メモリ
１２　第２メモリ
１４，２５，３６，４５，５４　ＣＰＵ
２１　リーダ／ライタ
２２　指紋読取器
３１，４２　暗号化／復号部
２４，３２，４３，５３　メモリ
３３，４４，５１　記憶装置
３５　入力部
４１　指紋スキャナ
５２　通信部

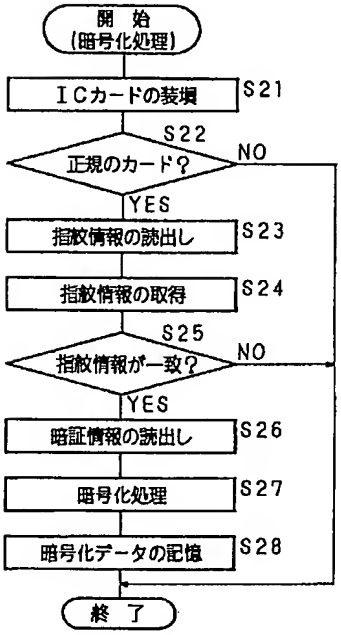
【図１】


1
ICカード
CPU
14
13
インタフェース
11
第1メモリ
12
第2メモリ
2
不正アクセス防止装置
CPU
25
21
リーダ/ライタ
24
メモリ
23
インタフェース
22
指紋読取器
3
コンピュータ
CPU
36
32
メモリ
31
暗号化/復号部
33
記憶装置
34
インタフェース
35
入力部

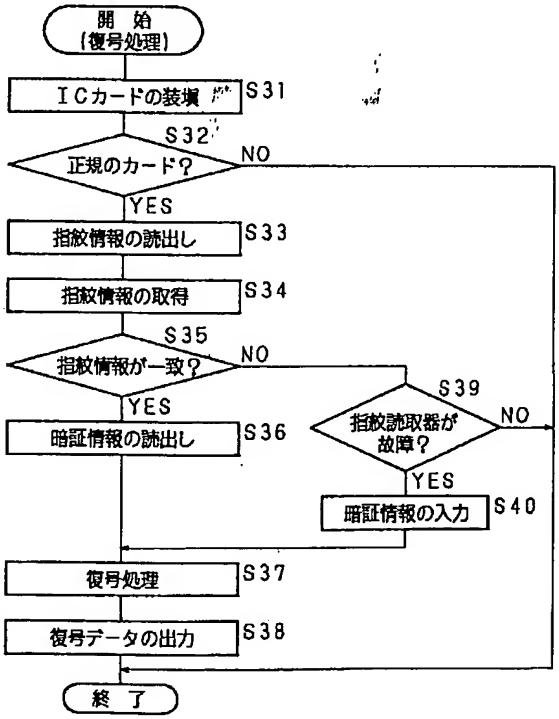
【図２】


開始
(登録処理)
指紋情報の取得・ICカードへの書込み
S11
暗証情報の設定・ICカードへの書込み
S12
暗証情報の登録
S13
指紋情報及び暗証情報の緊急復元カードへの書込み
S14
終了

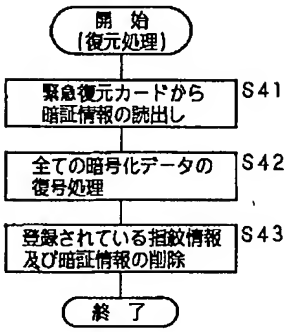
【図３】


開始
(暗号化処理)
ICカードの装填
S21
正規のカード?
S22
NO
YES
指紋情報の読出し
S23
指紋情報の取得
S24
指紋情報が一致?
S25
NO
YES
暗証情報の読出し
S26
暗号化処理
S27
暗号化データの記憶
S28
終了

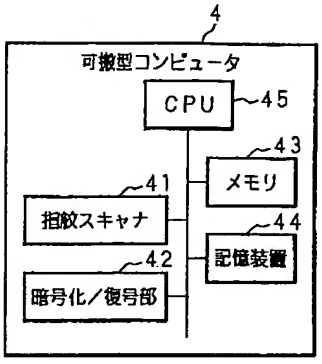
【図４】


開始
(復号処理)
ICカードの装填
S31
正規のカード?
S32
NO
YES
指紋情報の読出し
S33
指紋情報の取得
S34
指紋情報が一致?
S35
NO
YES
暗証情報の読出し
S36
指紋読取器が故障?
S39
NO
YES
暗証情報の入力
S40
復号処理
S37
復号データの出力
S38
終了

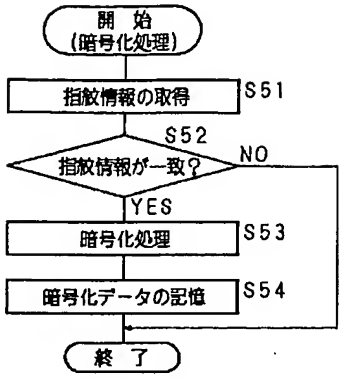
【図５】


開始
(復元処理)
緊急復元カードから暗証情報の読出し
S41
全ての暗号化データの復号処理
S42
登録されている指紋情報及び暗証情報の削除
S43
終了

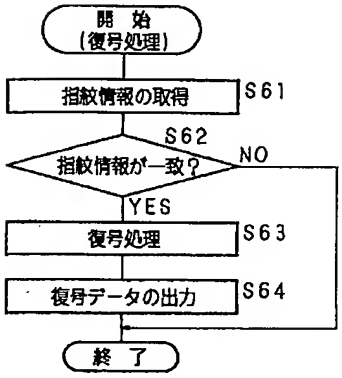
【図６】



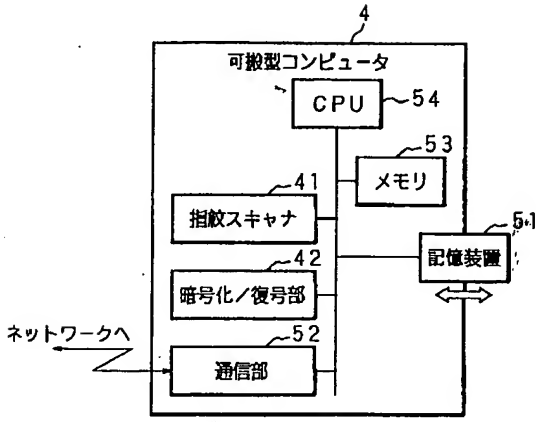
【図７】



【図８】



【図９】



フロントページの続き

(51)Int.Cl.'		識別記号	FI		テーマコード (参考)
G06F	12/00	537	G06F	9/06	660E 5J104
G06K	19/10		G06K	19/00	S
	19/00				T
H04L	9/32		H04L	9/00	673A
					673D
					673E